CSUN INFORMATION TECHNOLOGY	Vulnerability Management Procedure For Servers February 16, 2017

Overview

This document clarifies the campus procedure for vulnerability management, including scanning, assessment, and remediation of the discovered vulnerabilities for CSUN servers. The results of the vulnerability scans help inform server administrators of known and potential vulnerabilities, so those vulnerabilities can be remediated.

A vulnerability is a security exposure in an operating system or other system software or application software component including, but not limited to: missing operating system and application patches, inappropriately installed or active applications and services, software flaws and exploits, misconfigurations in systems, etc.

Related Polices and Standards

- CSU Information Security Policy - 8000.00 - Introduction and Scope
- CSU Information Security Policy - 8045.00 - Information Technology Security
- CSU Information Security Standard - 8045.S500 - Information Asset Monitoring

Vulnerability Assessment

No new server shall be migrated and considered to be in production until a vulnerability assessment has been conducted and vulnerabilities addressed.

Vulnerability assessments must be performed:

- Just prior to moving any server into production.
- Monthly for all servers, or at a timeframe deemed appropriate by the ISO based upon the risk.
- Just prior to moving major upgrades or changes to any server into production.

Vulnerability Scanning Process

1. Campus server owners must notify the Information Security Office (using the IT Help Center ticketing system or via email to iso@csun.edu) of all new servers before they are migrated into production.
2. Campus server owners must notify the Information Security Office of all major upgrades or changes to any server before the changes are put into production.
3. The Information Security Office will conduct vulnerability scans for servers and share findings with server owners for review and, if necessary, remediation. The Information Security Office will work with the server owners to schedule the most appropriate time to conduct the vulnerability scans.
4. Servers must be scanned using authentication; therefore, the server owner must provide User ID credentials to the Information Security Office. The Information Security Office will submit a request for the account, specifying the level of access needed to scan the server.
5. Vulnerability scan reports will be placed in a secure myCSUNbox folder unique to each server owner and an email notification sent to the server owner.

6. When CSUN is notified of an off-cycle critical patch released by a vendor to mitigate a vulnerability, the ISO will notify all affected server owners of the necessity to implement the patch or remove the server from the network until the relevant patch is applied.
7. Vendor-maintained servers are subject to the same policies and standards as CSUN hosted servers. Vendors should provide to the owning department an audited attestation that they follow a vulnerability management and patching process, such as SSAE16 or PCI certification.

Remediation Process

At the completion of each vulnerability scan, campus server owners must review the vulnerability report and ensure that vulnerabilities are remediated.

Discovered vulnerabilities must be remediated on the following timeframes:

- Severity 5 and Severity 4 vulnerabilities - within 30 calendar days of discovery.
- Severity 3 vulnerabilities - within 90 calendar days of discovery.
- Severity 2 and Severity 1 vulnerabilities - within 180 calendar days of discovery.

If a server is found to be non-compliant and the problem is not resolved in the above referenced timeframe, the server may be removed from the campus network. Exceptions must be approved by the Information Security Officer.